IN THE CLAIMS:

1. (Currently Amended) A method of securing data stored on an electronic device, the method comprising:

encrypting the data using a cryptographic key derivable from or accessed using a passphrase;[[,]]

requiring the entry into the device of the passphrase when a user wishes to access the data;[[,]]

subsequently inhibiting access to the data whilst the device remains active;[[,]] and

requiring the entry into the device of a predefined password when a user wishes to access the data following inhibition of data access, the password being different from the passphrase, wherein, if the user fails to enter the correct password within a predefined number of attempts, the cryptographic key stored by the device is deleted or re-encrypted.

2. (Currently Amended) A method according to claim 1, wherein, ~~following inhibition of data access, the device requires that the user enter the correct password within a predefined number of attempts, and, if the user fails to enter the correct password within this number of attempts, the cryptographic key stored by the device is deleted~~ in the event that the user fails to enter the correct password within a predefined number of attempts, ~~and~~ the user is requested to reenter the correct passphrase.

3. (Currently Amended) A method according to claim 2, wherein, if the correct passphrase is not reentered by the user following failure by the user to enter the correct password, the encrypted data may only be accessed by entering the cryptographic key into the device.

4. (Original) A method according to claim 1 and comprising storing the predefined password in a memory of the device following encryption with said password or said cryptographic key, and verifying the password entered by the user by comparing it with the stored password.

5. (Currently Amended) A method of preventing unauthorised access to electronic data stored on a computer device, the method comprising:

requesting a user to input a passphrase into the device;

receiving an entered passphrase and using the passphrase to generate or access a cryptographic key;

storing the cryptographic key in a memory of the device, wherein the stored key can be used to subsequently encrypt and decrypt data on the device;

subsequently inhibiting a user from accessing data on the device after a predefined period, or after a predefined period of non-use, or after some predefined action by the user;

requesting a user to input a password into the device; and

receiving the password and, only if the password corresponds to a predefined password which is different from said passphrase, allowing the user to access data on

the device, otherwise ~~continuing to inhibit a user from accessing data on the device~~ deleting or re-encrypting the cryptographic key.

6. (Currently Amended) Apparatus for securing electronic data, the apparatus comprising:

a memory for storing encrypted and unencrypted data:

first processing means for encrypting data using a cryptographic key derivable from or accessed using a passphrase;

input means for receiving the passphrase from a user when the user wishes to access the data; and

second processing means for subsequently inhibiting access to the data whilst the device remains active, and for requiring the entry into the device of a predefined password via said input means when a user wishes to access the data, the password being different from the passphrase, and for causing the cryptographic key stored by the device to be deleted or re-encrypted if the user fails to enter the correct password within a predefined number of attempts.

7. (Original) Apparatus according to claim 6, the apparatus being a mobile computer device such as a laptop or palmtop computer, a PDA, or a mobile telephone.

8. (Currently Amended) A computer storage medium having stored thereon a program for causing a computer device to secure data stored on the electronic device by:

encrypting the data using a cryptographic key derivable from or accessed using a passphrase, requiring the entry into the device of the passphrase when a user wishes to access the data, subsequently inhibiting access to the data whilst the device remains active, and requiring the entry into the device of a predefined password when a user wishes to access the data, the password being different from the passphrase ~~password~~, and, in the event that the user fails to enter the correct password within a predefined number of attempts, deleting or re-encrypting the cryptographic key stored by the device.